Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch Interface Cards

Last Updated: July 01, 2011

This document provides configuration tasks for the 4-port Cisco HWIC-4ESW and the 9-port Cisco HWIC-D-9ESW EtherSwitch high-speed WAN interface cards (HWICs) hardware feature supported on Cisco 1800 (modular), Cisco 2800, and Cisco 3800 series integrated services routers.

Cisco EtherSwitch HWICs are 10/100BASE-T Layer 2 Ethernet switches with Layer 3 routing capability. (Layer 3 routing is forwarded to the host and is not actually performed at the switch.) Traffic between different VLANs on a switch is routed through the router platform. Any one port on a Cisco EtherSwitch HWIC may be configured as a stacking port to link to another Cisco EtherSwitch HWIC or EtherSwitch network module in the same system. An optional power module can also be added to provide inline power for IP telephones. The HWIC-D-9ESW HWIC requires a double-wide card slot.

This hardware feature does not introduce any new or modified Cisco IOS commands.

- Finding Feature Information, page 1
- Prerequisites for EtherSwitch HWICs, page 2
- Restrictions for EtherSwitch HWICs, page 2
- Prerequisites for Installing Two Ethernet Switch Network Modules in a Single Chassis, page 2
- Information About EtherSwitch HWICs, page 3
- How to Configure EtherSwitch HWICs , page 6
- Configuration Examples for EtherSwitch HWICs, page 105
- Additional References, page 116
- Feature Information for the Cisco HWIC-4ESW and the Cisco HWIC-D-9ESW EtherSwitch Cards, page 118

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information

about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EtherSwitch HWICs

The following are prerequisites to configuring EtherSwitch HWICs:

- Configuration of IP routing. See the *Cisco IOS IP Routing: Protocol-Independent Configuration Guide* for the Cisco IOS Release you are using.
- Use of the Cisco IOS T release, beginning with Release 12.3(8)T4 or later for Cisco HWIC-4ESW and Cisco HWIC-D-9ESW support. (See the Cisco IOS documentation.)

Restrictions for EtherSwitch HWICs

The following restrictions apply to the Cisco HWIC-4ESW and the Cisco HWIC-D-9ESW EtherSwitch HWICs:

- No more than two Ethernet Switch HWICs or network modules may be installed in a host router.

Multiple Ethernet Switch HWICs or network modules installed in a host router will not act independently of each other. They must be stacked, as they will not work at all otherwise.

- The ports of a Cisco EtherSwitch HWIC must NOT be connected to the Fast Ethernet/Gigabit onboard ports of the router.
- There is no inline power on the ninth port (port 8) of the HWIC-D-9ESW card.
- There is no Auto MDIX support on the ninth port (port 8) of the HWIC-D-9ESW card when either **speed** or **duplex** is not set to **auto**.
- There is no support for online insertion/removal (OIR) of the EtherSwitch HWICs.
- When Ethernet Switches have been installed and configured in a host router, OIR of the CompactFlash memory card in the router must not occur. OIR of the CompactFlash memory card will compromise the configuration of the Ethernet Switches.
- VTP pruning is not supported.
- There is a limit of 200 secure MAC addresses per module that can be supported by an EtherSwitch HWIC.
- Maximum traffic for a secure MAC address is 8 Mb/s.

Prerequisites for Installing Two Ethernet Switch Network Modules in a Single Chassis

A maximum of two Ethernet switch network modules can be installed in a single chassis. If two Ethernet switch network modules of any type are installed in the same chassis, the following configuration requirements must be met:

- Both Ethernet switch network modules must have an optional Gigabit Ethernet expansion board installed.

- An Ethernet crossover cable must be connected to the two Ethernet switch network modules using the optional Gigabit Ethernet expansion board ports.
- Intrachassis stacking for the optional Gigabit Ethernet expansion board ports must be configured. For information about intrachassis stacking configuration, see the 16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series module.

Note Without this configuration and connection, duplications will occur in the VLAN databases, and unexpected packet handling may occur.

Information About EtherSwitch HWICs

- VLANs, page 3
- Inline Power for Cisco IP Phones, page 3
- Layer 2 Ethernet Switching, page 3
- 802.1x Authentication, page 3
- Spanning Tree Protocol, page 4
- Cisco Discovery Protocol, page 4
- Switched Port Analyzer, page 4
- IGMP Snooping, page 4
- Storm Control, page 4
- Intrachassis Stacking, page 4
- Fallback Bridging, page 4
- Default 802.1x Configuration, page 4

VLANs

For conceptual information about VLANs, see the “VLANs” section of the EtherSwitch Network Module .

Inline Power for Cisco IP Phones

For conceptual information about inline power for Cisco IP phones, see the “Inline Power for Cisco IP Phones” section of the EtherSwitch Network Module

Layer 2 Ethernet Switching

For conceptual information about Layer 2 Ethernet switching, see the “Layer 2 Ethernet Switching” section of the EtherSwitch Network Module .

802.1x Authentication

For conceptual information about 802.1x authentication, see the “802.1x Authentication” section of the EtherSwitch Network Module .

Spanning Tree Protocol

For conceptual information about Spanning Tree Protocol, see the “Using the Spanning Tree Protocol with the EtherSwitch Network Module” section of the EtherSwitch Network Module .

Cisco Discovery Protocol

For conceptual information about Cisco Discovery Protocol, see the “Cisco Discovery Protocol” section of the EtherSwitch Network Module .

Switched Port Analyzer

For conceptual information about a switched port analyzer, see the “Switched Port Analyzer” section of the EtherSwitch Network Module .

IGMP Snooping

For conceptual information about IGMP snooping, see the “IGMP Snooping” section of the EtherSwitch Network Module.

Storm Control

For conceptual information about storm control, see the “Storm Control” section of the EtherSwitch Network Module .

Intrachassis Stacking

For conceptual information about intrachassis stacking, see the ‘Intrachassis Stacking” section of the EtherSwitch Network Module .

Fallback Bridging

For conceptual information about fallback bridging, see the “Fallback Bridging” section of the EtherSwitch Network Module .

Default 802.1x Configuration

The table below shows the default 802.1x configuration.

Table 1 Default 802.1x Configuration

Feature	Default Setting
Authentication, authorization, and accounting (AAA)	Disabled.

Feature	Default Setting
RADIUS server • IP address • UDP authentication port • Key	• None specified. • 1645. • None specified.
Per-interface 802.1x enable state	Disabled (force-authorized). The port transmits and receives normal traffic without 802.1x-based authentication of the client.
Periodic reauthentication	Disabled.
Number of seconds between reauthentication attempts	3600 seconds.
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).
Retransmission time	30 seconds (number of seconds that the switch should wait for a response to an EAP request/ identity frame from the client before retransmitting the request).
Maximum retransmission number	2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).
Multiple host support	Disabled.
Client timeout period	30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before retransmitting the request to the client). This setting is not configurable.
Authentication server timeout period	30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before retransmitting the response to the server). This setting is not configurable.

• 802.1x Configuration Guidelines, page 5

802.1x Configuration Guidelines

These are the 802.1x authentication configuration guidelines:

- When the 802.1x protocol is enabled, ports are authenticated before any other Layer 2 feature is enabled.

- The 802.1x protocol is supported on Layer 2 static-access ports, but it is not supported on these port types:
  - Trunk port--If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.
  - Switch Port Analyzer (SPAN) destination port--You can enable 802.1x on a port that is a SPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. You can enable 802.1x on a SPAN source port.

How to Configure EtherSwitch HWICs

- Configuring VLANs , page 6
- Configuring VLAN Trunking Protocol, page 8
- Configuring Layer 2 Interfaces, page 12
- Configuring 802.1x Authentication, page 21
- Configuring Spanning Tree, page 33
- Configuring MAC Table Manipulation, page 43
- Configuring Cisco Discovery Protocol, page 46
- Configuring the Switched Port Analyzer (SPAN), page 50
- Configuring Power Management on the Interface, page 52
- Configuring IP Multicast Layer 3 Switching, page 54
- Configuring IGMP Snooping, page 58
- Configuring Per-Port Storm Control, page 64
- Configuring Stacking, page 67
- Configuring Fallback Bridging, page 69
- Configuring Separate Voice and Data Subnets, page 87
- Managing the EtherSwitch HWIC, page 90

Configuring VLANs

- Adding a VLAN Instance, page 6
- Deleting a VLAN Instance from the Database, page 7

Adding a VLAN Instance

A total of 15 VLANs can be supported by an EtherSwitch HWIC.

Follow the steps below to configure a Fast Ethernet interface as Layer 2 access.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vlan** *vlan-id*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Router#` **`vlan database`**	Enters VLAN configuration mode.
Step 3	**vlan** *vlan-id* **Example:** `Router(vlan)#` **`vlan 1`**	Adds an Ethernet VLAN. • Enter the VLAN number.
Step 4	**exit** **Example:** `Router(vlan)#` **`exit`**	Updates the VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode.

Deleting a VLAN Instance from the Database

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Follow the steps below to delete a VLAN from the database.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **no vlan** *vlan-id*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Router# vlan database`	Enters VLAN configuration mode.
Step 3	**no vlan** *vlan-id* **Example:** `Router(vlan)# no vlan 1`	Deletes an Ethernet VLAN. • Enter the VLAN number.
Step 4	**exit** **Example:** `Router(vlan)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode.

Configuring VLAN Trunking Protocol

Note VTP pruning is not supported by EtherSwitch HWICs.

- Configuring a VTP Server, page 8
- Configuring a VTP Client, page 10
- Disabling VTP (VTP Transparent Mode), page 11

Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network.

Follow the steps below to configure the switch as a VTP server.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vtp server**
4. **vtp domain** *domain -name*
5. **vtp password** *password -value*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Router# vlan database`	Enters VLAN configuration mode.
Step 3	**vtp server** **Example:** `Router(vlan)# vtp server`	Configures the switch as a VTP server.
Step 4	**vtp domain** *domain -name* **Example:** `Router(vlan)# vtp domain` *distantusers*	Defines the VTP domain name. • Enter the VTP domain name. Domain names can be a maximum of 32 characters.
Step 5	**vtp password** *password -value* **Example:** `Router(vlan)# vtp password` *philadelphia*	(Optional) Sets a VTP domain password • Enter a password. Passwords can be from 8 to 64 characters.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(vlan)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, exits VLAN configuration mode, and returns to privileged EXEC mode.

Configuring a VTP Client

When a switch is in VTP client mode, you cannot change the VLAN configuration on the switch. The client switch receives VTP updates from a VTP server in the management domain and modifies its configuration accordingly.

Follow the steps below to configure the switch as a VTP client.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vtp client**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Router#` **vlan database**	Enters VLAN configuration mode.
Step 3	**vtp client** **Example:** `Router(vlan)#` **vtp client**	Configures the switch as a VTP client.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(vlan)#` **exit**	Updates the VLAN database, propagates it throughout the administrative domain, exits VLAN configuration mode and returns to privileged EXEC mode.

Disabling VTP (VTP Transparent Mode)

When you configure the switch as VTP transparent, you disable VTP on the switch. A VTP transparent switch does not send VTP updates and does not act on VTP updates received from other switches.

Follow the steps below to disable VTP on the switch.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vtp transparent**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Router#` **vlan database**	Enters VLAN configuration mode.
Step 3	**vtp transparent** **Example:** `Router(vlan)#` **vtp transparent**	Configures VTP transparent mode.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(vlan)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, exits VLAN configuration mode, and returns to privileged EXEC mode.

Configuring Layer 2 Interfaces

- Configuring a Range of Interfaces, page 12
- Defining a Range Macro, page 13
- Configuring Layer 2 Optional Interface Features, page 14

Configuring a Range of Interfaces

Use the following task to configure a range of interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface range** {**macro** *macro-name* | **fastethernet** *interface-id* [**-** *interface-id*] | **vlan** *vlan-id*} [**,** **fastethernet** *interface-id* [- *interface-id*] | **vlan** *vlan-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface range** {**macro** *macro-name* | **fastethernet** *interface-id* [**-** *interface-id*] | **vlan** *vlan-id*} [**, fastethernet** *interface-id* [**-** *interface-id*] | **vlan** *vlan-id*] **Example:** `Router(config)# interface range FastEthernet 0/1/0 - 0/1/3`	Select the range of interfaces to be configured. • The space before the dash is required. For example, the command **interface range fastethernet**0/<*slot*>**/0 -**0/<*slot*>/**3** is valid; the command **interface range fastethernet**0/<*slot*>**/0-**0/<*slot*>/**3** is not valid. • You can enter one macro or up to five comma-separated ranges. • Comma-separated ranges can include both VLANs and physical interfaces. • You are not required to enter spaces before or after the comma. • The **interface range** command only supports VLAN interfaces that are configured with the **interface vlan** command.

Defining a Range Macro

Use the following task to define an interface range macro.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **define interface-range** *macro-name {* **fastethernet** *interface-id* [**-** *interface-id*] | {**vlan** *vlan-id* **-** *vlan-id*} | [**, fastethernet** *interface-id* [**-** *interface-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **define interface-range** *macro-name* { **fastethernet** *interface-id* [- *interface-id*] | {**vlan** *vlan-id* - *vlan-id*} | [**, fastethernet** *interface-id* [- *interface-id*] **Example:** `Router(config)# define interface-range first_three FastEthernet0/1/0 - 2`	Defines a range of macros. • Enter the macro name, along with the interface type and interface number, as appropriate.

Configuring Layer 2 Optional Interface Features

This section provides the following configuration information:

- Configuring the Interface Speed, page 12 (optional)
- Configuring the Interface Duplex Mode, page 13 (optional)
- Configuring a Description for an Interface, page 14 (optional)
- Configuring a Description for an Interface, page 14 (optional)
- Configuring a Fast Ethernet Interface as a Layer 2 Trunk, page 15 (optional)
- Configuring a Fast Ethernet Interface as Layer 2 Access, page 17 (optional)

- Configuring the Interface Speed, page 14
- Configuring the Interface Duplex Mode, page 15
- Configuring a Description for an Interface, page 17
- Configuring a Fast Ethernet Interface as a Layer 2 Trunk, page 17
- Configuring a Fast Ethernet Interface as Layer 2 Access, page 19

Configuring the Interface Speed

Use the following task to set the interface speed.

When configuring an interface speed, note these guidelines:

- If both ends of the line support autonegotiation, Cisco highly recommends the default auto negotiation settings.
- If one interface supports auto negotiation and the other end does not, configure interface speed on both interfaces; do not use the **auto** setting on the supported side.
- Both ends of the line need to be configured to the same setting; for example, both hard-set or both auto-negotiate. Mismatched settings are not supported.

Caution Changing the interface speed might shut down and reenable the interface during the reconfiguration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface fastethernet *interface-id*
4. **speed** {**10** | **100** | **1000** [**negotiate**] | **auto**[*speed-list*]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	interface fastethernet *interface-id* **Example:** `Router(config)# interface fastethernet 0/1/0`	Selects the interface to be configured and enters interface configuration mode. • Enter the interface number.
Step 4	**speed** {**10** | **100** | **1000** [**negotiate**] | **auto**[*speed-list*]} **Example:** `Router(config-if)# speed 100`	Configures the speed for the interface. • Enter the desired speed.

Note If you set the interface speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are automatically negotiated.

Configuring the Interface Duplex Mode

Follow the steps below to set the duplex mode of a Fast Ethernet interface.

When configuring an interface duplex mode, note these guidelines:

- If both ends of the line support autonegotiation, Cisco highly recommends the default auto negotiation settings.
- If one interface supports auto negotiation and the other end does not, configure duplex speed on both interfaces; do not use the **auto** setting on the supported side.

- Both ends of the line need to be configured to the same setting; for example, both hard-set or both auto-negotiate. Mismatched settings are not supported.

Caution Changing the interface duplex mode configuration might shut down and reenable the interface during the reconfiguration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface fastethernet *interface-id*
4. **duplex** [**auto** | **full** | **half**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	interface fastethernet *interface-id* **Example:** `Router(config)# interface fastethernet 0/1/0`	Selects the interface to be configured. • Enter the interface number.
Step 4	**duplex** [**auto**	**full**	**half**] **Example:** `Router(config-if)# duplex auto`	Sets the duplex mode of the interface.

Note If you set the port speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are automatically negotiated. You cannot change the duplex mode of auto negotiation interfaces.

Configuring a Description for an Interface

You can add a description of an interface to help you remember its function. The description appears in the output of the following commands: **show configuration**, **show running-config**, and **show interfaces**.

Use the **description**command to add a description for an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface fastethernet *interface-id*
4. **description** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	interface fastethernet *interface-id* **Example:** `Router(config)# interface fastethernet 0/1/0`	Selects the interface to be configured, and enters interface configuration mode. • Enter the interface number.
Step 4	**description** *string* **Example:** `Router(config-if)# description newinterface`	Adds a description for the interface. • Enter a description for the interface.

Configuring a Fast Ethernet Interface as a Layer 2 Trunk

Use this task to configure a Fast Ethernet interface as a Layer 2 trunk.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface fastethernet *interface-id*
4. **shutdown**
5. switchport **mode trunk**
6. switchport **trunk native vlan** *vlan-number*
7. switchport **trunk allowed vlan** {**add** | **except** | **none** | **remove**} *vlan1*[**,** *vlan*[**,** *vlan*[**,** ...]]
8. **no shutdown**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	interface fastethernet *interface-id* **Example:** `Router(config)#` **interface fastethernet 0/1/0**	Selects the interface to be configured and enters interface configuration mode. • Enter the interface number.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 5	switchport **mode trunk** **Example:** `Router(config-if)# switchport mode trunk`	Configures the interface as a Layer 2 trunk. **Note** Encapsulation is always dot1q.

	Command or Action	Purpose
Step 6	switchport **trunk native vlan** *vlan-number* **Example:** `Router(config-if)# switchport trunk native vlan 1`	(Optional) For 802.1Q trunks, specifies the native VLAN.
Step 7	switchport **trunk allowed vlan** {**add** | **except** | **none** | **remove**} *vlan1*[**,** *vlan*[**,** *vlan*[**,** ...]] **Example:** `Router(config-if)# switchport trunk allowed vlan add vlan1, vlan2, vlan3`	(Optional) Configures the list of VLANs allowed on the trunk. All VLANs are allowed by default. You cannot remove any of the default VLANs from a trunk.
Step 8	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the interface. (Required only if you shut down the interface.)
Step 9	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Note Ports do not support Dynamic Trunk Protocol (DTP). Ensure that the neighboring switch is set to a mode that will not send DTP.

Configuring a Fast Ethernet Interface as Layer 2 Access

Follow these steps below to configure a Fast Ethernet interface as Layer 2 access.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface fastethernet *interface-id*
4. **shutdown**
5. **switchport mode access**
6. **switchport access vlan** *vlan -number*
7. **no shutdown**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	interface fastethernet *interface-id* **Example:** `Router(config)# interface fastethernet 0/1/0`	Selects the interface to be configured and enters interface configuration mode. • Enter the interface number.
Step 4	**shutdown** **Example:** **Example:** `Router(config-if)# shutdown`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 5	**switchport mode access** **Example:** `Router(config-if)# switchport mode access`	Configures the interface as a Layer 2 access.
Step 6	**switchport access vlan** *vlan -number* **Example:** `Router(config-if)# switchport access vlan 1`	For access ports, specifies the access VLAN. • Enter the VLAN number.

	Command or Action	Purpose
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the interface. • Required only if you shut down the interface.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

Configuring 802.1x Authentication

- Enabling 802.1x Authentication, page 21
- Configuring the Switch-to-RADIUS-Server Communication, page 23
- Enabling Periodic Reauthentication, page 25
- Changing the Quiet Period, page 26
- Changing the Switch-to-Client Retransmission Time, page 28
- Setting the Switch-to-Client Frame-Retransmission Number, page 29
- Enabling Multiple Hosts, page 30
- Resetting the 802.1x Configuration to the Default Values, page 32
- Displaying 802.1x Statistics and Status, page 33

Enabling 802.1x Authentication

To enable 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

For additional information on default 802.1x configuration refer to the “Default 802.1x Configuration” section.

Complete these steps to configure 802.1x port-based authentication. This procedure is required.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*]
4. **interface** *interface-type interface-number*
5. **dot1x port-control auto**
6. **end**
7. **show dot1x**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication dot1x default newmethod`	Creates an 802.1x authentication method list. • To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • Enter at least one of these keywords: ◦ **group radius**--Use the list of all RADIUS servers for authentication. ◦ **none**--Use no authentication. The client is automatically authenticated without the switch using the information supplied by the client.
Step 4	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/1/3`	Specifies the interface to be enabled for 802.1x authentication and enters interface configuration mode. • Enter the interface type and interface number.

	Command or Action	Purpose
Step 5	**dot1x port-control auto** **Example:** `Router(config-if)# dot1x port-control auto`	Enables 802.1x on the interface. • For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports see the "802.1x Configuration Guidelines" section.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show dot1x** **Example:** `Router# show dot1x`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service--for example, authentication--the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string* **Example:** `Router(config)# radius-server host hostseven auth-port 75 key newauthority75`	Configures the RADIUS server parameters on the switch. • For *hostname* | *ip-address*,specify the host name or IP address of the remote RADIUS server. • For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1645. • For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. • If you want to use multiple RADIUS servers, repeat this command.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

To delete the specified RADIUS server, use the **no radius-server host** {*hostname* | *ip-address*} global configuration command.

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, refer to the RADIUS server documentation.

Enabling Periodic Reauthentication

You can enable periodic 802.1x client reauthentication and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication attempts is 3600 seconds.

Automatic 802.1x client reauthentication is a global setting and cannot be set for clients connected to individual ports.

Follow these steps to enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x re-authentication**
4. **dot1x timeout re-authperiod** *seconds*
5. **end**
6. **show dot1x**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot1x re-authentication** **Example:** `Router(config)# dot1x re-authentication`	Enables periodic reauthentication of the client. • Periodic reauthentication is disabled by default.
Step 4	**dot1x timeout re-authperiod** *seconds* **Example:** `Router(config)# dot1x timeout re-authperiod 120`	Sets the number of seconds between reauthentication attempts. • The range is 1 to 4294967295; the default is 3600 seconds. • This command affects the behavior of the switch only if periodic reauthentication is enabled
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 6	**show dot1x** **Example:** `Router# show dot1x`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time, and then tries again. The idle time is determined by the quiet-period value. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering smaller number than the default.

Follow these steps to change the quiet period.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x timeout quiet-period** *seconds*
4. **end**
5. **show dot1x**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot1x timeout quiet-period** *seconds* **Example:** `Router(config)#dot1x timeout quiet-period 120`	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. • The range is 0 to 65535 seconds; the default is 60.
Step 4	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show dot1x** **Example:** `Router# show dot1x`	Verifies your entries.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time), and then retransmits the frame.

Note You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Follow the steps below to change the amount of time that the switch waits for client notification.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x timeout tx-period** *seconds*
4. **end**
5. **show dot1x**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dot1x timeout tx-period** *seconds* **Example:** `Router(config)# dot1x timeout tx-period seconds`	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. • The range is 1 to 65535 seconds; the default is 30.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show dot1x** **Example:** `Router# show dot1x`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

Note You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Follow the steps below to set the switch-to-client frame-retransmission number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x max-req** *count*
4. **end**
5. **show dot1x**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot1x max-req** *count* **Example:** `Router(config)# dot1x max-req 5`	Sets the number of times that the switch sends an EAP-request/ identity frame to the client before restarting the authentication process. • The range is 1 to 10; the default is 2.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show dot1x** **Example:** `Router# show dot1x`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling Multiple Hosts

You can attach multiple hosts to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails, and an EAPOL-logoff message is received), all attached clients are denied access to the network.

Follow these steps below to allow multiple hosts (clients) on an 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **dot1x multiple-hosts**
5. **end**
6. **show dot1x**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/1/2`	Specifies the interface, and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**dot1x multiple-hosts** **Example:** `Router(config-if)# dot1x multiple-hosts`	Allows multiple hosts (clients) on an 802.1x-authorized port. • Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show dot1x** **Example:** `Router# show dot1x`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Resetting the 802.1x Configuration to the Default Values

You can reset the 802.1x configuration to the default values with a single command.

Follow these steps to reset the 802.1x configuration to the default values.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x default**
4. **end**
5. **show dot1x**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dot1x default** **Example:** `Router(config)# dot1x default`	Resets the configurable 802.1x parameters to the default values.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show dot1x** **Example:** `Router# show dot1x`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Displaying 802.1x Statistics and Status

To display 802.1x statistics for all interfaces, use the **show dot1x statistics** privileged EXEC command. To display 802.1x statistics for a specific interface, use the **show dot1x statistics interface** *interface-id*privileged EXEC command.

To display the 802.1x administrative and operational status for the switch, use the **show dot1x**privileged EXEC command. To display the 802.1x administrative and operational status for a specific interface, use the **show dot1x interface** *interface-id* privileged EXEC command.

Configuring Spanning Tree

- Enabling Spanning Tree, page 34
- Configuring Spanning Tree Port Priority, page 35
- Configuring Spanning Tree Port Cost, page 36
- Configuring the Bridge Priority of a VLAN, page 38
- Configuring Hello Time, page 39
- Configuring the Forward-Delay Time for a VLAN, page 40
- Configuring the Maximum Aging Time for a VLAN, page 40
- Configuring the Root Bridge, page 41

Enabling Spanning Tree

You can enable spanning tree on a per-VLAN basis. The switch maintains a separate instance of spanning tree for each VLAN (except on VLANs on which you disable spanning tree).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **spanning -tree vlan** *vlan-id*
4. **end**
5. **show spanning-tree vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**spanning -tree vlan** *vlan-id* **Example:** `Router(config)# spanning-tree vlan 200`	Enables spanning tree on a per-VLAN basis • Enter the VLAN number.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show spanning-tree vlan** *vlan-id* **Example:** `Router# show spanning-tree vlan 200`	Verifies spanning tree configuration. • Enter the VLAN number.

Configuring Spanning Tree Port Priority

Follow the steps below to configure the spanning tree port priority of an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet**} *interface-id*
4. **spanning -tree port-priority** *port-priority*
5. **spanning -tree vlan** *vlan-id* **port-priority** *port-priority*
6. **end**
7. **show spanning-tree interface fastethernet** *interface-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet**	**fastethernet**} *interface-id* **Example:** `Router(config)# interface fastethernet 0/1/6`	Selects an interface to configure, and enters interface configuration mode. • Enter the interface number.
Step 4	**spanning -tree port-priority** *port-priority* **Example:** `Router(config-if)# spanning-tree port-priority 8`	Configures the port priority for an interface. • The of port-priority *value* can be from 4 to 252 in increments of 4. • Use the **no** form of this command to restore the defaults.
Step 5	**spanning -tree vlan** *vlan-id* **port-priority** *port-priority* **Example:** `Router (config-if)# spanning-tree vlan vlan1 port-priority 12`	Configures the priority for a VLAN.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 7	**show spanning-tree interface fastethernet** *interface-id* **Example:** `Router# show spanning-tree interface fastethernet 0/1/6`	(Optional) Saves your entries in the configuration file.

Configuring Spanning Tree Port Cost

Spanning tree port costs are explained in the following section.

Port cost value calculations are based on the bandwidth of the port. There are two classes of values. Short (16-bit) values are specified by the IEEE 802.1D specification and range in value from 1 to 65535. Long (32-bit) values are specified by the IEEE 802.1t specification and range in value from 1 to 200,000,000.

Assigning Short Port Cost Values

You can manually assign port costs in the range of 1 to 65535. Default cost values are listed in the table below.

Table 2 Default Cost Values

Port Speed	Default Cost Value
10 Mbps	100
100 Mbps	19

Assigning Long Port Cost Values

You can manually assign port costs in the range of 1 to 200,000,000. Recommended cost values are listed in the table below.

Table 3 Recommended Cost Values

Port Speed	Recommended Value	Recommended Range
10 Mbps	2,000,000	200,000 to 20,000,000
100 Mbps	200,000	20,000 to 2,000,000

Follow the steps below to configure the spanning tree port cost of an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet**} *interface-id*
4. **spanning -tree cost** *port-cost*
5. **spanning -tree vlan** *vlan-id* **cost** *port-cost*
6. **end**
7. **show spanning-tree interface fastethernet** *interface-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet**	**fastethernet**} *interface-id* **Example:** `Router(config)# interface fastethernet 0/1/6`	Selects an interface to configure, and enters interface configuration mode. • Enter the interface number.
Step 4	**spanning -tree cost** *port-cost* **Example:** `Router(config-if)# spanning-tree cost 2000`	Configures the port cost for an interface. • The value of port-cost can be from 1 to 200,000,000 (1 to 65,535 in Cisco IOS Releases 12.1(2)E and earlier). • Use the **no** form of this command to restore the defaults.
Step 5	**spanning -tree vlan** *vlan-id* **cost** *port-cost* **Example:** `Router(config-if)# spanning-tree vlan 200 cost 2000`	Configures the VLAN port cost for an interface. • The value port-cost can be from 1 to 65,535. • Use the **no** form of this command to restore the defaults.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 7	**show spanning-tree interface fastethernet** *interface-id* **Example:** `Router# show spanning-tree interface fastethernet 0/1/6`	(Optional) Saves your entries in the configuration file.

Configuring the Bridge Priority of a VLAN

Use the following task to configure the spanning tree bridge priority of a VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **spanning -tree vlan** *vlan-id* **priority** *bridge-priority*
4. **show spanning-tree vlan bridge**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **spanning -tree vlan** *vlan-id* **priority** *bridge-priority* **Example:** `Router(config)# spanning-tree vlan 200 priority 2`	Configures the bridge priority of a VLAN. The *bridge-priority* value can be from 0 to 65535. • Use the **no** form of this command to restore the defaults. **Caution** Exercise care when using this command. For most situations **spanning-tree vlan vlan-id root primary** and the **spanning-tree vlan vlan-id root secondary** are the preferred commands to modify the bridge priority.
Step 4 **show spanning-tree vlan bridge** **Example:** `Router(config-if)# spanning-tree cost 200`	Verifies the bridge priority.

Configuring Hello Time

Use the following tasks to configure the hello interval for the spanning tree.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **spanning -tree vlan** *vlan-id* **hello-time** *hello-time*

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 **configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**spanning -tree vlan** *vlan-id* **hello-time** *hello-time* **Example:** `Router(config)# spanning-tree vlan 200 hello-time 5`	Configures the hello time of a VLAN. • Enter the VLAN number. • The **hello-time** value can be from 1 to 10 seconds. • Use the **no** form of this command to restore the defaults

Configuring the Forward-Delay Time for a VLAN

Use the following task to configure the forward delay for the spanning tree.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **spanning - tree vlan** *vlan -id* **forward - time** *forward-time*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**spanning - tree vlan** *vlan -id* **forward - time** *forward-time* **Example:** `Router(config)# spanning-tree vlan 20 forward-time 5`	Configures the forward time of a VLAN. • Enter the VLAN number. • The value of *forward-time* can be from 4 to 30 seconds. • Use the **no** form of this command to restore the defaults.

Configuring the Maximum Aging Time for a VLAN

Follow the steps below to configure the maximum age interval for the spanning tree.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **spanning -tree vlan** *vlan-id* **max-age** *max-age*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**spanning -tree vlan** *vlan-id* **max-age** *max-age* **Example:** `Router(config)# spanning-tree vlan 200 max-age 30`	Configures the maximum aging time of a VLAN. • Enter the VLAN number. • The value of *max-age* can be from 6 to 40 seconds. • Use the **no** form of this command to restore the defaults.

Configuring the Root Bridge

The EtherSwitch HWIC maintains a separate instance of spanning tree for each active VLAN configured on the switch. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID will become the root bridge for that VLAN.

To configure a VLAN instance to become the root bridge, the bridge priority can be modified from the default value (32768) to a significantly lower value so that the bridge becomes the root bridge for the specified VLAN. Use the **spanning-tree vlan root** command to alter the bridge priority.

The switch checks the bridge priority of the current root bridges for each VLAN. The bridge priority for the specified VLANs is set to 8192 if this value will cause the switch to become the root for the specified VLANs.

If any root switch for the specified VLANs has a bridge priority lower than 8192, the switch sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

For example, if all switches in the network have the bridge priority for VLAN 100 set to the default value of 32768, entering the spanning-tree vlan 100 root primary command on a switch will set the bridge priority for VLAN 100 to 8192, causing the switch to become the root bridge for VLAN 100.

Note The root switch for each instance of spanning tree should be a backbone or distribution switch. Do not configure an access switch as the spanning tree primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically picks an optimal hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the spanning tree convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

Note We recommend that you avoid configuring the hello time, forward delay time, and maximum age time manually after configuring the switch as the root bridge.

Follow these steps to configure the switch as the root.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **spanning tree vlan** *vlan id* **root primary** [**diameter** *hops* [**hell o- time** *seconds*]]
4. **no spanning -tree vlan** *vlan-id*
5. **show spanning -tree vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**spanning tree vlan** *vlan id* **root primary** [**diameter** *hops* [**hell o- time** *seconds*]] **Example:** `Router(config)# spanning-tree vlan 200 root primary`	Configures a switch as the root switch. • Enter the VLAN number, along with any optional keywords or arguments as needed.

	Command or Action	Purpose
Step 4	**no spanning -tree vlan** *vlan-id* **Example:** `Router(config)# spanning-tree vlan 200 root primary`	Disables spanning tree on a per-VLAN basis. • Enter the VLAN number.
Step 5	**show spanning -tree vlan** *vlan-id* **Example:** `Router(config)# show spanning-tree vlan 200`	Verifies spanning tree on a per-VLAN basis. • Enter the VLAN number.

Configuring MAC Table Manipulation

Port security is implemented by providing the user with the option to make a port secure by allowing only well-known MAC addresses to send in data traffic. Up to 200 secure MAC addresses per HWIC are supported.

- Enabling Known MAC Address Traffic, page 43
- Creating a Static Entry in the MAC Address Table, page 44
- Configuring and Verifying the Aging Timer, page 45

Enabling Known MAC Address Traffic

Follow these steps to enable the MAC address secure option.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **m ac-address-table secure** *mac -address* **fastethernet** *interface-id* [**vlan** *vlan-id*]]
4. **end**
5. **show mac-address-table secure**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**m ac-address-table secure** *mac -address* **fastethernet** *interface-id* [**vlan** *vlan-id*]] **Example:** `Router(config)# mac-address-table secure 0000.0002.0001 fastethernet 0/1/1 vlan 2`	Secures the MAC address traffic on the port. • Enter the MAC address, the **fastethernet** keyword, the interface number and any optional keywords and arguments as desired.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show mac-address-table secure** **Example:** `Router# show mac-address-table secure`	Verifies the configuration.

Creating a Static Entry in the MAC Address Table

Follow these steps to create a static entry in the MAC address table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **mac-address - table static** *mac-address* **fastethernet** *interface-id* [**vlan** *vlan-id*]
4. **end**
5. **show mac-address-table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router(config)# **mac-address - table static** *mac-address* **fastethernet** *interface-id* [**vlan** *vlan-id*] **Example:** `Router(config)# mac-address-table static 00ff.ff0d. 2dc0 fastethernet 0/1/1`	Creates a static entry in the MAC address table. • When the *vlan-id* is not specified, VLAN 1 is taken by default.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show mac-address-table** **Example:** `Router# show mac-address-table`	Verifies the MAC address table.

Configuring and Verifying the Aging Timer

The aging timer may be configured from 16 seconds to 4080 seconds, in 16-second increments.

Follow these steps to configure the aging timer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac -address-table aging-tim e** *time*
4. **end**
5. **show mac-address-table aging-time**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mac -address-table aging-tim e** *time* **Example:** `Router(config)# mac-address-table aging-time 4080`	Configures the MAC address aging timer age in seconds. • The range is 0 to 10000 seconds.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show mac-address-table aging-time** **Example:** `Router# show mac-address-table aging-time`	Verifies the MAC address table.

Configuring Cisco Discovery Protocol

- Enabling Cisco Discovery Protocol, page 46
- Enabling CDP on an Interface, page 47
- Monitoring and Maintaining CDP, page 49

Enabling Cisco Discovery Protocol

To enable Cisco Discovery Protocol (CDP) globally, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp run**
4. **end**
5. **show cdp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cdp run** **Example:** `Router(config)# cdp run`	Enables CDP globally.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show cdp** **Example:** `Router# show cdp`	Verifies the CDP configuration.

Enabling CDP on an Interface

Use the steps below to enable CDP on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet**} *interface-id*
4. **cdp enable**
5. **end**
6. **show cdp interface** *interface-id*
7. **show cdp neighbors**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet**	**fastethernet**} *interface-id* **Example:** `Router(config)# interface fastethernet 0/1/1`	Selects an interface to configure, and enters interface configuration mode. • Enter the interface number.
Step 4	**cdp enable** **Example:** `Router(config-if)# cdp enable`	Enables CDP globally.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

	Command or Action	Purpose
Step 6	**show cdp interface** *interface-id* **Example:** `Router# show cdp interface`	Verifies the CDP configuration on the interface.
Step 7	**show cdp neighbors** **Example:** `Router# show cdp neighbors`	Verifies the information about the neighboring equipment.

Monitoring and Maintaining CDP

Use the following commands to monitor and maintain CDP on your device.

SUMMARY STEPS

1. **enable**
2. **clear cdp counter** s
3. **clear cdp table**
4. **show cdp**
5. **show cdp entry** *entry-name* [**protocol** | **version**]
6. **show cdp interface** *interface-id*
7. **show cdp neighbors** *interface-id* [**detail**]
8. **show cdp traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear cdp counter** s **Example:** `Router# clear cdp counters`	(Optional) Resets the traffic counters to zero.

	Command or Action	Purpose
Step 3	**clear cdp table** **Example:** `Router# clear cdp table`	(Optional) Deletes the CDP table of information about neighbors.
Step 4	**show cdp** **Example:** `Router# show cdp`	(Optional) Verifies global information such as frequency of transmissions and the holdtime for packets being transmitted.
Step 5	**show cdp entry** *entry-name* [**protocol** | **version**] **Example:** `Router# show cdp entry newentry`	(Optional) Verifies information about a specific neighbor. • The display can be limited to protocol or version information.
Step 6	**show cdp interface** *interface-id* **Example:** `Router# show cdp interface 0/1/1`	(Optional) Verifies information about interfaces on which CDP is enabled. • Enter the interface number.
Step 7	**show cdp neighbors** *interface-id* [**detail**] **Example:** `Router# show cdp neighbors 0/1/1`	(Optional) Verifies information about neighbors. • The display can be limited to neighbors on a specific interface and can be expanded to provide more detailed information.
Step 8	**show cdp traffic** **Example:** `Router# show cdp traffic`	(Optional) Verifies CDP counters, including the number of packets sent and received and checksum errors.

Configuring the Switched Port Analyzer (SPAN)

Note An EtherSwitch HWIC supports only one SPAN session. Either Tx or both Tx and Rx monitoring is supported.

- Configuring the SPAN Sources, page 51
- Configuring SPAN Destinations, page 51

Configuring the SPAN Sources

Use the following task to configure the source for a SPAN session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session 1** {**source** {**interface** *interface-id*} | {**vlan** *vlan-id*}} [**,** | **-** | **rx** | **tx** | **both**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor session 1** {**source** {**interface** *interface-id*} | {**vlan** *vlan-id*}} [**,** | **-** | **rx** | **tx** | **both**] **Example:** `Router(config)# monitor session 1 source interface fastethernet 0/3/1`	Specifies the SPAN session (number 1), the source interfaces or VLANs, and the traffic direction to be monitored. • The example shows how to configure the SPAN session to monitor bidirectional traffic from source interface Fast Ethernet 0/3/1.

Configuring SPAN Destinations

To configure the destination for a SPAN session, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *session-id* {**destination** {**interface** *interface-id*} | {**vlan** *vlan-id*}} [, | - | **rx** | **tx** | **both**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *session-id* {**destination** {**interface** *interface-id*} | {**vlan** *vlan-id*}} [, | - | **rx** | **tx** | **both**] **Example:** `Router(config)# monitor session 1 source interface fastethernet 0/3/1`	Specifies the SPAN session (number 1), the source interfaces or VLANs, and the traffic direction to be monitored. • The example shows how to configure the SPAN session to monitor bidirectional traffic from source interface Fast Ethernet 0/3/1.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring Power Management on the Interface

The HWICs can supply inline power to a Cisco 7960 IP phone, if necessary. The Cisco 7960 IP phone can also be connected to an AC power source and supply its own power to the voice circuit. When the Cisco 7960 IP phone is supplying its own power, an HWICs can forward IP voice traffic to and from the phone.

A detection mechanism on the HWIC determines whether it is connected to a Cisco 7960 IP phone. If the switch senses that there is no power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch never to supply power to the Cisco 7960 IP phone and to disable the detection mechanism.

Follow these steps to manage the powering of the Cisco IP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface fastethernet** *interface-id*
4. **power inline** {**auto** |**never**}
5. **end**
6. **show power inline**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface fastethernet** *interface-id* **Example:** `Router(config)# interface fastethernet 0/3/1`	Selects a particular Fast Ethernet interface for configuration, and enters interface configuration mode. • Enter the interface number.
Step 4	**power inline** {**auto** |**never**} **Example:** `Router(config-if)# power inline auto`	Configures the port to supply inline power automatically to a Cisco IP phone. • Use **never** to permanently disable inline power on the port.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show power inline** **Example:** `Router# show power inline`	Displays power configuration on the ports.

Configuring IP Multicast Layer 3 Switching

- Enabling IP Multicast Routing Globally, page 54
- Enabling IP Protocol-Independent Multicast (PIM) on Layer 3 Interfaces, page 55
- Verifying IP Multicast Layer 3 Hardware Switching Summary, page 56
- Verifying the IP Multicast Routing Table, page 58

Enabling IP Multicast Routing Globally

You must enable IP multicast routing globally before you can enable IP multicast Layer 3 switching on Layer 3 interfaces.

For complete information and procedures, see the following publications:

- *Cisco IOS IP Routing: Protocol-Independent Configuration Guide*
- *Cisco IOS IP Addressing Services Command Reference*
- *Cisco IOS IP Routing: Protocol-Independent Command Reference*

Note See the Cisco command reference listing page for protocol-specific command references.

- *Cisco IOS IP Multicast Command Reference*

Use the following commands to enable IP multicast routing globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing globally.

Enabling IP Protocol-Independent Multicast (PIM) on Layer 3 Interfaces

You must enable protocol-independent multicast (PIM) on the Layer 3 interfaces before enabling IP multicast Layer 3 switching functions on those interfaces.

Beginning in global configuration mode, follow these steps to enable IP PIM on a Layer 3 interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan** *vlan-id*
4. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan** *vlan-id* **Example:** **Example:** `Router(config)# interface vlan 1`	Selects the interface to be configured and enters interface configuration mode.
Step 4	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} **Example:** `Router(config-if)# ip pim sparse-dense mode`	Enables IP PIM on a Layer 3 interface.

Verifying IP Multicast Layer 3 Hardware Switching Summary

Note The **show interface statistics** command does not verify hardware-switched packets, only packets switched by software.

The **show ip pim interface count**command verifies the IP multicast Layer 3 switching enable state on IP PIM interfaces and verifies the number of packets received and sent on the interface.

Use the following **show** commands to verify IP multicast Layer 3 switching information for an IP PIM Layer 3 interface.

SUMMARY STEPS

1. Router# show ip pim interface count
2. Router# show ip mroute count
3. Router# show ip interface vlan 1

DETAILED STEPS

Step 1 Router# show ip pim interface count

Example:

```
State:* - Fast Switched, D - Distributed Fast Switched
      H - Hardware Switching Enabled
Address          Interface            FS  Mpackets In/Out
10.0.0.1         VLAN1                *   151/0
Router#
```

Step 2 Router# show ip mroute count

Example:

```
IP Multicast Statistics
5 routes using 2728 bytes of memory
4 groups, 0.25 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:209.165.200.225 Source count:1, Packets forwarded: 0, Packets received: 66
  Source:10.0.0.2/32, Forwarding:0/0/0/0, Other:66/0/66
Group:209.165.200.226, Source count:0, Packets forwarded: 0, Packets received: 0
Group:209.165.200.227, Source count:0, Packets forwarded: 0, Packets received: 0
Group:209.165.200.228, Source count:0, Packets forwarded: 0, Packets received: 0
Router#
```

Note A negative counter means that the outgoing interface list of the corresponding entry is NULL, and this indicates that this flow is still active.

Step 3 Router# show ip interface vlan 1

Example:

```
Vlan1 is up, line protocol is up
  Internet address is 10.0.0.1/24
  Broadcast address is 209.165.201.1
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined:209.165.201.2 209.165.201.3 209.165.201.4 209.165.201.5
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
```

```
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
Router#
```

Verifying the IP Multicast Routing Table

Use the **show ip mroute**command to verify the IP multicast routing table:

```
Router# show ip mroute 224.10.103.10
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched, A - Assert winner
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode
(*, 209.165.201.2), 00:09:21/00:02:56, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse-Dense, 00:09:21/00:00:00, H
Router#
```

Note The RPF-MFD flag indicates that the flow is completely hardware switched. The H flag indicates that the flow is hardware-switched on the outgoing interface.

Configuring IGMP Snooping

- Enabling or Disabling IGMP Snooping, page 58
- Enabling IGMP Immediate-Leave Processing, page 60
- Statically Configuring an Interface to Join a Group, page 61
- Configuring a Multicast Router Port, page 63

Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the EtherSwitch HWIC. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. By default, IGMP snooping is enabled on all VLANs, but it can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the per-VLAN IGMP snooping capability. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable snooping on a VLAN basis.

Follow the steps below to globally enable IGMP snooping on the EtherSwitch HWIC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping**
4.
5. **ip igmp snooping vlan** *vlan-id*
6. **end**
7. **show ip igmp snooping**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping** **Example:** `Router(config)# ip igmp snooping`	Globally enables IGMP snooping in all existing VLAN interfaces.
Step 4		
Step 5	**ip igmp snooping vlan** *vlan-id* **Example:** `Router(config)# ip igmp snooping vlan 100`	Globally enables IGMP snooping on a specific VLAN interface. • Enter the VLAN number.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 7	**show ip igmp snooping** **Example:** `Router# show ip igmp snooping`	Displays snooping configuration.
Step 8	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your configuration to the startup configuration.

Enabling IGMP Immediate-Leave Processing

When you enable IGMP Immediate-Leave processing, the EtherSwitch HWIC immediately removes a port from the IP multicast group when it detects an IGMP version 2 Leave message on that port. Immediate-Leave processing allows the switch to remove an interface that sends a Leave message from the forwarding table without first sending out group-specific queries to the interface. You should use the Immediate-Leave feature only when there is only a single receiver present on every port in the VLAN.

Use the following steps to enable IGMP Immediate-Leave processing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id* **immediate-leave**
4. **end**
5. **show ip igmp snooping**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **immediate-leave** **Example:** `Router(config)# ip igmp snooping vlan 1 immediate-leave`	Enables IGMP Immediate-Leave processing on the VLAN interface. • Enter the VLAN number.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip igmp snooping** **Example:** `Router# show ip igmp snooping`	Displays snooping configuration.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your configuration to the startup configuration.

Statically Configuring an Interface to Join a Group

Ports normally join multicast groups through the IGMP report message, but you can also statically configure a host on an interface.

Follow the steps below to add a port as a member of a multicast group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id*
4. **end**
5. **show mac-address-table multicast** [**vlan** *vlan-id*] [**user**| **igmp-snooping**] [**count**]
6. **show ip igmp snooping**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* **Example:** `Router(config)# ip igmp snooping vlan 1 static 0100.5e05.0505 interface Fa0/1/1`	Enables IGMP snooping on the VLAN interface.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show mac-address-table multicast** [**vlan** *vlan-id*] [**user**| **igmp-snooping**] [**count**] **Example:** `Router# show mac-address-table multicast vlan 1 igmp-snooping`	Displays MAC address table entries for a VLAN. • *vlan-id* is the multicast group VLAN ID. • **user** displays only the user-configured multicast entries. • **igmp-snooping** displays entries learned via IGMP snooping. • **count** displays only the total number of entries for the selected criteria, not the actual entries.
Step 6	**show ip igmp snooping** **Example:** `Router# show ip igmp snooping`	Displays snooping configuration.

	Command or Action	Purpose
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your configuration to the startup configuration.

Configuring a Multicast Router Port

Follow the steps below to enable a static connection to a multicast router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}
4. **end**
5. **show ip igmp snooping**
6. **show ip igmp snooping mrouter** [**vlan** *vlan-id*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id*	**learn pim-dvmrp**} **Example:** `Router(config)# ip igmp snooping vlan1 interface Fa0/1/1 learn pim-dvmrp`	Enables IGMP snooping on the VLAN interface and enables route discovery.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip igmp snooping** **Example:** `Router# show ip igmp snooping`	(Optional) Displays snooping configuration.
Step 6	**show ip igmp snooping mrouter** [**vlan** *vlan-id*] **Example:** `Router# show ip igmp snooping mroute vlan vlan1`	(Optional) Displays Mroute discovery information.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your configuration to the startup configuration.

Configuring Per-Port Storm Control

You can use these techniques to block the forwarding of unnecessary flooded traffic.

By default, unicast, broadcast, and multicast suppression is disabled.

- Enabling Per-Port Storm Control, page 64
- Disabling Per-Port Storm Control, page 66

Enabling Per-Port Storm Control

Use these steps to enable per-port storm control.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** *level-high* [**level-low**]
5. **storm-control action shutdown**
6. **end**
7. **show storm-control** [**interface**] [**broadcast** | **multicast** | **unicast** | **history**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/3/1`	Specifies the port to configure, and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** *level-high* [**level-low**] **Example:** `Router(config-if)# Storm-control broadcast level 7`	Configures broadcast, multicast, or unicast per-port storm control. • Specify the rising threshold level for either broadcast, multicast, or unicast traffic. The storm control action occurs when traffic utilization reaches this level. • (Optional) Specify the falling threshold level. The normal transmission restarts (if the action is filtering) when traffic drops below this level.
Step 5	**storm-control action shutdown** **Example:** `Router(config-if)# Storm-control action shutdown`	Selects the **shutdown** keyword to disable the port during a storm. • The default is to filter out the traffic.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 7	**show storm-control** [**interface**] [**broadcast** | **multicast** | **unicast** | **history**] **Example:** `Router# show storm-control`	(Optional) Verifies your entries.

Note If any type of traffic exceeds the upper threshold limit, all of the other types of traffic will be stopped.

Disabling Per-Port Storm Control

Follow these steps to disable per-port storm control.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **no storm-control** {**broadcast** | **multicast**| **unicast**} **level** *level-high* [*level-low*]
5. **no storm-control action shutdown**
6. **end**
7. **show storm-control** [**interface**] [{**broadcast** | **multicast** | **unicast** | **history**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/3/1`	Specifies the port to configure, and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**no storm-control** {**broadcast** | **multicast**| **unicast**} **level** *level-high* [*level-low*] **Example:** `Router(config-if)# no storm-control broadcast level 7`	Disables per-port storm control.
Step 5	**no storm-control action shutdown** **Example:** `Router(config-if)# no storm-control action shutdown`	Disables the specified storm control action.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show storm-control** [**interface**] [{**broadcast** | **multicast** | **unicast** | **history**}] **Example:** `Router# show storm-control`	(Optional) Verifies your entries.

Configuring Stacking

Stacking is the connection of two switch modules resident in the same chassis so that they behave as a single switch. When a chassis is populated with two switch modules, the user must configure both of them to operate in stacked mode. This is done by selecting one port from each switch module and configuring it to be a stacking partner. The user must then use a cable to connect the stacking partners from each switch module to physically stack the switch modules. Any one port in a switch module can be designated as the stacking partner for that switch module.

Follow the steps below to configure a pair of ports on two different switch modules as stacking partners.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface fastethernet** *interface-id*
4. **no shutdown**
5. **switchport stacking-partner interface fastethernet** *partner-interface-id*
6. **exit**
7. **interface** fastethernet *partner-interface-id*
8. **no shutdown**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface fastethernet** *interface-id* **Example:** `Router(config)# interface fastethernet 0/3/1`	Specifies the port to configure and enters interface configuration mode. • Enter the interface number.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the interface. • This step is required only if you shut down the interface.
Step 5	**switchport stacking-partner interface fastethernet** *partner-interface-id* **Example:** `Router(config-if)# switchport stacking-partner interface FastEthernet partner-interface-id`	Selects and configures the stacking partner port. • Enter the partner interface number. • To restore the defaults, use the **no** form of this command.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to privileged configuration mode.
Step 7	**interface** fastethernet *partner-interface-id* **Example:** `Router# interface fastethernet 0/3/1`	Specifies the partner-interface, and enters interface configuration mode. • Enter the partner interface number.
Step 8	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the stacking partner interface.
Step 9	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

Note Both stacking partner ports must have their **speed** and **duplex** parameters set to **auto**.

Caution If stacking is removed, stacked interfaces will go to **shutdown** state. Other nonstacked ports will be left unchanged.

Configuring Fallback Bridging

The table below shows the default fallback bridging configuration.

Table 4 Default Fallback Bridging Configuration

Feature	Default Setting
Bridge groups	None are defined or assigned to an interface. No VLAN-bridge STP is defined.
Switch forwards frames for stations that it has dynamically learned	Enabled.

Feature	Default Setting
Bridge table aging time for dynamic entries	300 seconds.
MAC-layer frame filtering	Disabled.
Spanning tree parameters: • Switch priority • Interface priority • Interface path cost • Hello BPDU interval • Forward-delay interval • Maximum idle interval	• 32768 • 128 • 10 Mbps: 100 100 Mbps: 19 1000 Mbps: 4 • 2 seconds • 20 seconds • 30 seconds

- Creating a Bridge Group, page 70
- Preventing the Forwarding of Dynamically Learned Stations, page 72
- Configuring the Bridge Table Aging Time, page 73
- Filtering Frames by a Specific MAC Address, page 75
- Adjusting Spanning-Tree Parameters, page 76
- Adjusting BPDU Intervals, page 81
- Monitoring and Maintaining the Network, page 86

Creating a Bridge Group

To configure fallback bridging for a set of switched virtual interfaces (SVIs), these interfaces must be assigned to bridge groups. All interfaces in the same group belong to the same bridge domain. Each SVI can be assigned to only one bridge group.

Follow the steps below to create a bridge group and assign an interface to it.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip routing**
4. **bridge** *bridge-group* **protocol vlan-bridge**
5. **interface** *interface-type interface-number*
6. **bridge-group** *bridge-group*
7. **end**
8. **show vlan-bridge**
9. **show running-config**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no ip routing** **Example:** `Router(config)# no ip routing`	Disables IP routing.
Step 4	**bridge** *bridge-group* **protocol vlan-bridge** **Example:** `Router(config)# bridge 100 protocol vlan-bridge`	Assigns a bridge group number and specifies the VLAN-bridge spanning-tree protocol to run in the bridge group. • The **ibm** and **dec** keywords are not supported. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • Frames are bridged only among interfaces in the same group.
Step 5	**interface** *interface-type interface-number* **Example:** `Router(config)# interface vlan 0/3/1`	Specifies the interface on which you want to assign the bridge group, and enters interface configuration mode. • The specified interface must be an SVI: a VLAN interface that you created by using the **interface vlan** *vlan-id* global configuration command. • These ports must have IP addresses assigned to them.
Step 6	**bridge-group** *bridge-group* **Example:** `Router(config-if)# bridge-group 100`	Assigns the interface to the bridge group created in Step 4 . • By default, the interface is not assigned to any bridge group. An interface can be assigned to only one bridge group.
Step 7	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	**show vlan-bridge** **Example:** `Router# show vlan-bridge`	(Optional) Verifies forwarding mode.
Step 9	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entries.
Step 10	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Preventing the Forwarding of Dynamically Learned Stations

By default, the switch forwards any frames for stations that it has dynamically learned. When this activity is disabled, the switch only forwards frames whose addresses have been statically configured into the forwarding cache.

Follow the steps below to prevent the switch from forwarding frames for stations that it has dynamically learned.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no bridge** *bridge-group* **acquire**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no bridge** *bridge-group* **acquire** **Example:** **Example:** `Router(config)# no bridge 100 acquire`	Enables the switch to stop forwarding any frames for stations that it has dynamically learned through the discovery process and to limit frame forwarding to statically configured stations. • The switch filters all frames except those whose destined-to addresses have been statically configured into the forwarding cache. To configure a static address, use the **bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} global configuration command. • For *bridge-group*, specify the bridge group number. The range is 1 to 255.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Configuring the Bridge Table Aging Time

A switch forwards, floods, or drops packets based on the bridge table. The bridge table maintains both static and dynamic entries. Static entries are entered by you. Dynamic entries are entered by the bridge learning process. A dynamic entry is automatically removed after a specified length of time, known as aging time, from the time the entry was created or last updated.

If you are likely to move hosts on a switched network, decrease the aging time to enable the switch to quickly adapt to the change. If hosts on a switched network do not continuously send packets, increase the aging time to keep the dynamic entries for a longer time and thus reduce the possibility of flooding when the hosts send again.

Follow the steps below to configure the aging time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **aging-time** *seconds*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bridge** *bridge-group* **aging-time** *seconds* **Example:** `Router(config)# bridge 100 aging-time 10000`	Specifies the length of time that a dynamic entry remains in the bridge table from the time the entry was created or last updated. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 0 to 1000000. The default is 300 seconds.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Filtering Frames by a Specific MAC Address

A switch examines frames and sends them through the internetwork according to the destination address; a switch does not forward a frame back to its originating network segment. You can use the software to configure specific administrative filters that filter frames based on information other than the paths to their destinations.

You can filter frames with a particular MAC-layer station destination address. Any number of addresses can be configured in the system without a performance penalty.

Follow the steps below to filter by the MAC-layer address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-id*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-id*] **Example:** **Example:** `Router(config)# bridge 1 address 0800.cb00.45e9 forward ethernet 1`	Filters frames with a particular MAC-layer station source or destination address. • Enter the bridge-group number (the range is 1 to 255), the MAC address and the **forward** or **discard** keywords.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Adjusting Spanning-Tree Parameters

You might need to adjust certain spanning-tree parameters if the default values are not suitable for your switch configuration. Parameters affecting the entire spanning tree are configured with variations of the **bridge** global configuration command. Interface-specific parameters are configured with variations of the **bridge-group** interface configuration command.

You can adjust spanning-tree parameters by performing any of the tasks in these sections:

- Changing the Switch Priority, page 67
- Changing the Interface Priority, page 68
- Assigning a Path Cost, page 69
- Adjusting BPDU Intervals, page 71
- Adjusting the Interval Between Hello BPDUs, page 71
- Changing the Forward-Delay Interval, page 72
- Changing the Maximum-Idle Interval, page 73
- Disabling the Spanning Tree on an Interface, page 74

Note Only network administrators with a good understanding of how switches and STP function should make adjustments to spanning-tree parameters. Poorly planned adjustments can have a negative impact on performance.

- Changing the Switch Priority, page 77
- Changing the Interface Priority, page 78
- Assigning a Path Cost, page 79

Changing the Switch Priority

You can globally configure the priority of an individual switch when two switches tie for position as the root switch, or you can configure the likelihood that a switch will be selected as the root switch. This priority is determined by default; however, you can change it.

Follow the steps below to change the switch priority.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **priority** *number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bridge** *bridge-group* **priority** *number* **Example:** `Router(config)# bridge 100 priority 5`	Changes the priority of the switch. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *number*, enter a number from 0 to 65535. The default is 32768. The lower the number, the more likely the switch will be chosen as the root.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	Verifies your entry.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Changing the Interface Priority

You can change the priority for an interface. When two switches tie for position as the root switch, you configure an interface priority to break the tie. The switch with the lower interface value is elected.

Follow the steps below to change the interface priority.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **bridge** *bridge-group* **priority** *number*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/3/1`	Specifies the interface to set the priority, and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**bridge** *bridge-group* **priority** *number* **Example:** `Router(config-if)# bridge 100 priority 4`	Changes the priority of the bridge. • Enter the bridge-group number and the priority number.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Assigning a Path Cost

Each interface has a path cost associated with it. By convention, the path cost is 1000/data rate of the attached LAN, in Mbps.

Follow the steps below to assign a path cost.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **bridge** *bridge-group* **path-costs** *cost*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/3/1`	Specifies the interface to set the priority and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**bridge** *bridge-group* **path-costs** *cost* **Example:** `Router(config-if)# bridge 100 pathcost 4`	Changes the path cost. • Enter the bridge-group number and cost.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Adjusting BPDU Intervals

You can adjust bridge protocol data unit (BPDU) intervals as described in these sections:

- Adjusting the Interval Between Hello BPDUs, page 71 (optional)
- Changing the Forward-Delay Interval, page 72 (optional)
- Changing the Maximum-Idle Interval, page 73 (optional)

Note Each switch in a spanning tree adopts the interval between hello BPDUs, the forward delay interval, and the maximum idle interval parameters of the root switch, regardless of what its individual configuration might be.

- Adjusting the Interval Between Hello BPDUs, page 81
- Changing the Forward-Delay Interval, page 82
- Changing the Maximum-Idle Interval, page 84
- Disabling the Spanning Tree on an Interface, page 85

Adjusting the Interval Between Hello BPDUs

Follow the steps below to adjust the interval between hello BPDUs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **hello-time** *seconds*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bridge** *bridge-group* **hello-time** *seconds* **Example:** `Router(config)# bridge 100 hello-time 5`	Specifies the interval between hello BPDUs. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 1 to 10. The default is 2 seconds.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Changing the Forward-Delay Interval

The forward-delay interval is the amount of time spent listening for topology change information after an interface has been activated for switching and before forwarding actually begins.

Follow the steps below to change the forward-delay interval.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **forward-time** *seconds*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bridge** *bridge-group* **forward-time** *seconds* **Example:** `Router(config)# bridge 100 forward-time 25`	Specifies the forward-delay interval. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 10 to 200. The default is 20 seconds.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.

Command or Action	Purpose
Step 6 **copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Changing the Maximum-Idle Interval

If a switch does not hear BPDUs from the root switch within a specified interval, it recomputes the spanning-tree topology.

Follow the steps below to change the maximum-idle interval (maximum aging time).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **max-age** *seconds*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 **configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3 **bridge** *bridge-group* **max-age** *seconds* **Example:** `Router(config)# bridge 100 forward-time 25`	Specifies the interval the switch waits to hear BPDUs from the root switch. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 10 to 200. The default is 30 seconds.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Disabling the Spanning Tree on an Interface

When a loop-free path exists between any two switched subnetworks, you can prevent BPDUs generated in one switching subnetwork from impacting devices in the other switching subnetwork, yet still permit switching throughout the network as a whole. For example, when switched LAN subnetworks are separated by a WAN, BPDUs can be prevented from traveling across the WAN link.

Follow the steps below to disable spanning tree on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **bridge-group** *bridge-group* **spanning-disabled**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/3/1`	Specifies the interface to set the priority and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**bridge-group** *bridge-group* **spanning-disabled** **Example:** `Router(config-if)# bridge 100 spanning-disabled`	Disables spanning tree on the interface. • For *bridge-group*, specify the bridge group number. The range is 1 to 255.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies your entry.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

Monitoring and Maintaining the Network

To monitor and maintain the network, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **clear bridge** *bridge-group*
3. **show bridge**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear bridge** *bridge-group* **Example:** `Router# clear bridge bridge1`	(Optional) Removes any learned entries from the forwarding database and clears the transmit and receive counts for any statically configured entries. • Enter the number of the bridge group.
Step 3	**show bridge** **Example:** `Router# show bridge`	(Optional) Displays classes of entries in the bridge forwarding database.
Step 4	**end** **Example:** `Router# end`	(Optional) Exits privileged EXEC mode.

Configuring Separate Voice and Data Subnets

The HWICs can automatically configure voice VLAN. This capability overcomes the management complexity of overlaying a voice topology onto a data network while maintaining the quality of voice traffic. With the automatically configured voice VLAN feature, network administrators can segment phones into separate logical networks, even though the data and voice infrastructure is physically the same. The voice VLAN feature places the phones into their own VLANs without the need for end-user intervention. A user can plug the phone into the switch, and the switch provides the phone with the necessary VLAN information.

For ease of network administration and increased scalability, network managers can configure the HWICs to support Cisco IP phones such that the voice and data traffic reside on separate subnets. You should

always use separate VLANs when you are able to segment the existing IP address space of your branch office.

User priority bits in the 802.1p portion of the 802.1Q standard header are used to provide prioritization in Ethernet switches. This is a vital component in designing Cisco AVVID networks.

The HWICs provides the performance and intelligent services of Cisco IOS software for branch office applications. The HWICs can identify user applications--such as voice or multicast video--and classify traffic with the appropriate priority levels.

Follow these steps to automatically configure Cisco IP phones to send voice traffic on the voice VLAN ID (VVID) on a per-port basis (see the “Voice Traffic and VVID” section).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **switchport mode trunk**
5. **switchport voice vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/2/1`	Specifies the port to be configured and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	**switchport mode trunk** **Example:** `Router(config-if)# switchport mode trunk`	Configures the port to trunk mode.

	Command or Action	Purpose
Step 5	**switchport voice vlan** *vlan-id* **Example:** `Router(config-if)# switchport voice vlan 100`	Configures the voice port with a VVID that will be used exclusively for voice traffic. • Enter the VLAN number.

• Configuring a Single Subnet for Voice and Data, page 89

Configuring a Single Subnet for Voice and Data

For network designs with incremental IP telephony deployment, network managers can configure the HWICs so that the voice and data traffic coexist on the same subnet. This might be necessary when it is impractical either to allocate an additional IP subnet for IP phones or to divide the existing IP address space into an additional subnet at the remote branch, it might be necessary to use a single IP address space for branch offices. (This is one of the simpler ways to deploy IP telephony.)

This configuration approach must address two key considerations:

- Network managers should ensure that existing subnets have enough available IP addresses for the new Cisco IP phones, each of which requires a unique IP address.
- Administering a network with a mix of IP phones and workstations on the same subnet might pose a challenge.

Follow these steps to automatically configure Cisco IP phones to send voice and data traffic on the same VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. switchport access vlan vlan-id
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface fastethernet 0/2/1`	Specifies the port to be configured, and enters interface configuration mode. • Enter the interface type and interface number.
Step 4	switchport access vlan vlan-id **Example:** `Router(config-if)# switchport access vlan 100`	Sets the native VLAN for untagged traffic. • The value of *vlan-id* represents the ID of the VLAN that is sending and receiving untagged traffic on the port. Valid IDs are from 1 to 1001. Leading zeroes are not permitted.
Step 5	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Managing the EtherSwitch HWIC

- Adding Trap Managers, page 90
- Configuring IP Information, page 91
- Enabling Switch Port Analyzer, page 95
- Managing the ARP Table, page 97
- Managing the MAC Address Tables, page 97
- Removing Dynamic Addresses, page 99
- Adding Secure Addresses, page 100
- Removing a Secure Address, page 101
- Configuring Static Addresses, page 102
- Removing a Static Address, page 103
- Clearing All MAC Address Tables, page 104

Adding Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, community strings for each member switch must be unique. If a member switch has an IP address assigned to it, the management station accesses the switch by using its assigned IP address.

By default, no trap manager is defined, and no traps are issued.

Follow these steps to add a trap manager and community string.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *ip-address traps* **snmp** *vlan-membership*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**snmp-server host** *ip-address traps* **snmp** *vlan-membership*
	
	Example:
	`Router(config)#`
	`snmp-server host 172.16.128.263 traps1 snmp`
	`vlancommunity1`
		Enters the trap manager IP address, community string, and the traps to generate.

Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring IP Information

This section describes how to assign IP information on the HWICs. The following topics are included:

- Assigning IP Information to the Switch, page 80
- Removing IP Information From a Switch, page 81
- Specifying a Domain Name and Configuring the DNS, page 82

- Assigning IP Information to the Switch, page 92
- Removing IP Information From a Switch, page 93
- Specifying a Domain Name and Configuring the DNS, page 95

Assigning IP Information to the Switch

You can use a BOOTP server to automatically assign IP information to the switch; however, the BOOTP server must be set up in advance with a database of physical MAC addresses and corresponding IP addresses, subnet masks, and default gateway addresses. In addition, the switch must be able to access the BOOTP server through one of its ports. At startup, a switch without an IP address requests the information from the BOOTP server; the requested information is saved in the switch running the configuration file. To ensure that the IP information is saved when the switch is restarted, save the configuration by entering the **write memory** command in privileged EXEC mode.

You can change the information in these fields. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

Follow these steps to enter the IP information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. ip address ip-address subnet-mask
5. **exit**
6. ip default-gateway ip-address
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface vlan 1`	Specifies the interface (in this case, the VLAN) to which the IP information is assigned and enters interface configuration mode. • Enter the interface type and interface number. • VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.
Step 4	ip address ip-address subnet-mask **Example:** `Router(config-if)# ip address 192.168.2.10 255.255.255.255`	Specifies the IP address. • Enter the IP address and subnet mask.
Step 5	**exit** **Example:** `Router(config)# exit`	Returns to global configuration mode.
Step 6	ip default-gateway ip-address **Example:** `Router# ip default-gateway 192.168.2.20`	Sets the IP address of the default router. • Enter the IP address of the default router.
Step 7	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Removing IP Information From a Switch

Use the following procedure to remove the IP information (such as an IP address) from a switch.

Note Using the **no ip address** command in interface configuration mode disables the IP protocol stack and removes the IP information. Cluster members without IP addresses rely on the IP protocol stack being enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **no ip address**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface vlan 1`	Specifies the interface (in this case, the VLAN) to which the IP information is assigned and enters interface configuration mode. • Enter the interface type and interface number. • VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Removes the IP address and subnet mask.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Danger If you are removing the IP address through a telnet session, your connection to the switch will be lost .

Specifying a Domain Name and Configuring the DNS

Each unique IP address can have a host name associated with it. The Cisco IOS software maintains an EXEC mode and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the FTP system, for example, is identified as *ftp.cisco.com*.

To track domain names, IP has defined the concept of a domain name server (DNS), the purpose of which is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet's global naming scheme that uniquely identifies network devices.

Specifying the Domain Name

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name has that domain name appended to it before being added to the host table.

Specifying a Name Server

You can specify up to six hosts that can function as a name server to supply name information for the DNS.

Enabling the DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet's global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

Enabling Switch Port Analyzer

You can monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A Switch Port Analyzer (SPAN) port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. Any number of ports can be defined as SPAN ports, and any combination of ports can be monitored. SPAN is supported for up to 2 sessions.

Follow the steps below to enable SPAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** session-id {**destination** | **source**} {**interface** | **vlan** *interface-id* | *vlan-id*}} [**,** | **-** | **both** | **tx** | **rx**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** session-id {**destination** | **source**} {**interface** | **vlan** *interface-id* | *vlan-id*}} [**,** | **-** | **both** | **tx** | **rx**] **Example:** `Router(config)# monitor session session-id {destination | source} {interface | vlan interface-id | vlan-id}} [, | - | both | tx | rx]`	Enables port monitoring for a specific session (*"number"*). • Optionally, supply a SPAN *destination* interface and a *source* interface.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

• Disabling SPAN, page 96

Disabling SPAN

Follow these steps to disable SPAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. no monitor session session-id
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	no monitor session session-id **Example:** `Router(config)# no monitor session 37`	Disables port monitoring for a specific session.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Managing the ARP Table

To communicate with a device (on Ethernet, for example), the software first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

When you manually add entries to the ARP table by using the CLI, you must be aware that these entries do not age and must be manually removed.

Managing the MAC Address Tables

This section describes how to manage the MAC address tables on the HWICs. The following topics are included:

- Understanding MAC Addresses and VLANs
- Changing the Address Aging Time
- Configuring the Aging Time

The switch uses the MAC address tables to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include the following types of addresses:

- Dynamic address--A source MAC address that the switch learns and then drops when it is not in use.
- Secure address--A manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
- Static address--A manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address. The following shows an example of a list of addresses as they would appear in the dynamic, secure, or static address table.

```
Router# show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
000a.000b.000c          Secure      1      FastEthernet0/1/8
000d.e105.cc70          Self        1      Vlan1
00aa.00bb.00cc          Static      1      FastEthernet0/1/0
```

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. Use the Aging Time field to define how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Follow these steps to configure the dynamic address table aging time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. mac-address-table aging-time seconds
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	mac-address-table aging-time seconds **Example:** `Router(config)# mac-address-table aging-time 30000`	Enters the number of seconds that dynamic addresses are to be retained in the address table. • Valid entries are from 10 to 1000000.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Removing Dynamic Addresses

Follow these steps to remove a dynamic address entry.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. no mac-address-table dynamic hw-addr
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	no mac-address-table dynamic hw-addr **Example:** `Router(config)# no mac-address-table dynamic 0100.5e05.0505`	Enters the MAC address to be removed from dynamic MAC address table.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

You can enter a secure port address even when the port does not yet belong to a VLAN. When the port is later assigned to a VLAN, packets destined for that address are forwarded to the port.

Note When you change the VLAN ID for a port that is configured with a secure MAC address, you must reconfigure the secure MAC address to reflect the new VLAN association.

Follow these steps to add a secure address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. mac-address-table secure **address** hw-addr **interface** *interface-id*vlan vlan-id
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	mac-address-table secure **address** hw-addr **interface** *interface-id*vlan vlan-id **Example:** `Router(config)# mac-address-table secure address 0100.5e05.0505 interface 0/3/1 vlan vlan 1`	Enters the MAC address, its associated port, and the VLAN ID.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Removing a Secure Address

Follow these steps to remove a secure address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. no mac-address-table secure hw-addr vlan vlan-id
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	no mac-address-table secure hw-addr vlan vlan-id **Example:** `Router(config)# no mac-address-table secure address 0100.5e05.0505 vlan vlan 1`	Enters the secure MAC address, its associated port, and the VLAN ID to be removed.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map. A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

Follow these steps to add a static address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. mac-address-table static hw-addr [interface] interface-id [vlan] vlan-id
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	mac-address-table static hw-addr [interface] interface-id [vlan] vlan-id **Example:** `Router(config)# mac-address-table static 0100.5e05.0505 interface 0/3/1 vlan vlan 1`	Enters the static MAC address, the interface, and the VLAN ID of those ports.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Removing a Static Address

Follow these steps to remove a static address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. no mac-address-table static hw-addr [interface] interface-id [vlan] vlan-id
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	no mac-address-table static hw-addr [interface] interface-id [vlan] vlan-id **Example:** `Router(config)# no mac-address-table static 0100.5e05.0505 interface 0/3/1 vlan vlan`	Enters the static MAC address, the interface, and the VLAN ID of the port to be removed.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Clearing All MAC Address Tables

Follow these steps to remove all MAC address tables.

SUMMARY STEPS

1. **enable**
2. **clear mac-address-table**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear mac-address-table** **Example:** `Router# clear mac-address-table`	Clears all MAC address tables.
Step 3	**end** **Example:** `Router# end`	Exits privileged EXEC mode.

Configuration Examples for EtherSwitch HWICs

- Range of Interface Examples, page 105
- Optional Interface Feature Examples, page 106
- Stacking Example, page 107
- VLAN Configuration Example, page 107
- VLAN Trunking Using VTP Example, page 107
- Spanning Tree Examples, page 108
- MAC Table Manipulation Example, page 111
- Switched Port Analyzer (SPAN) Source Examples, page 112
- IGMP Snooping Example, page 112
- Storm-Control Example, page 114
- Ethernet Switching Examples, page 114

Range of Interface Examples

- Single Range Configuration: Example, page 92
- Range Macro Definition: Example, page 92

- Single Range Configuration Example, page 106
- Range Macro Definition Example, page 106

Single Range Configuration Example

The following example shows all Fast Ethernet interfaces on an HWIC-4ESW in slot 2 being reenabled:

```
Router(config)# interface range fastethernet 0/3/0 - 8
Router(config-if-range)# no shutdown
Router(config-if-range)#
*Mar  21 14:01:21.474: %LINK-3-UPDOWN: Interface FastEthernet0/3/0, changed state to up
*Mar  21 14:01:21.490: %LINK-3-UPDOWN: Interface FastEthernet0/3/1, changed state to up
*Mar  21 14:01:21.502: %LINK-3-UPDOWN: Interface FastEthernet0/3/2, changed state to up
*Mar  21 14:01:21.518: %LINK-3-UPDOWN: Interface FastEthernet0/3/3, changed state to up
*Mar  21 14:01:21.534: %LINK-3-UPDOWN: Interface FastEthernet0/3/4, changed state to up
*Mar  21 14:01:21.546: %LINK-3-UPDOWN: Interface FastEthernet0/3/5, changed state to up
*Mar  21 14:01:21.562: %LINK-3-UPDOWN: Interface FastEthernet0/3/6, changed state to up
*Mar  21 14:01:21.574: %LINK-3-UPDOWN: Interface FastEthernet0/3/7, changed state to up
*Mar  21 14:01:21.590: %LINK-3-UPDOWN: Interface FastEthernet0/3/8, changed state to up
Router(config-if-range)#
```

Range Macro Definition Example

The following example shows an interface-range macro named enet_list being defined to select Fast Ethernet interfaces 0/1/0 through 0/1/3:

```
Router(config)# define interface-range enet_list fastethernet 0/1/0 - 0/1/3Router(config)#
```

The following example shows how to change to the interface-range configuration mode using the interface-range macro enet_list:

```
Router(config)# interface
 range
 macro
 enet
_list
```

Optional Interface Feature Examples

- Interface Speed: Example, page 93
- Setting the Interface Duplex Mode: Example, page 93
- Adding a Description for an Interface: Example, page 93
- Interface Speed Example, page 106
- Setting the Interface Duplex Mode Example, page 106
- Adding a Description for an Interface Example, page 107

Interface Speed Example

The following example shows the interface speed being set to 100 Mbps on Fast Ethernet interface 0/3/7:

```
Router(config)# interface fastethernet 0/3/7
Router(config-if)# speed 100
```

Setting the Interface Duplex Mode Example

The following example shows the interface duplex mode being set to full on Fast Ethernet interface 0/3/7:

```
Router(config)# interface fastethernet 0/3/7
Router(config-if)# duplex full
```

Adding a Description for an Interface Example

The following example shows how to add a description of Fast Ethernet interface 0/3/7:

```
Router(config)# interface fastethernet 0/3/7
Router(config-if)# description Link to root switch
```

Stacking Example

The following example shows how to stack two HWICs.

```
Router(config)# interface FastEthernet 0/1/8
Router(config-if)# no shutdown
Router(config-if)# switchport stacking-partner interface FastEthernet 0/3/8
Router(config-if)# interface FastEthernet 0/3/8
Router(config-if)# no shutdown
```

Note In practice, the command **switchport stacking-partner interface FastEthernet** *0/partner-slot/partner-port* needs to be executed for only one of the stacked ports. The other port will be automatically configured as a stacking port by the Cisco IOS software. The command **no shutdown**, however, must be executed for both of the stacked ports.

VLAN Configuration Example

The following example shows how to configure inter-VLAN routing:

```
Router# vlan database
Router(vlan)# vlan 1
Router(vlan)# vlan 2
Router(vlan)# exit
Router# configure terminal
Router(config)# interface vlan 1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface vlan 2
Router(config-if)# ip address 10.2.2.2 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface FastEthernet 0/1/0
Router(config-if)# switchport access vlan 1
Router(config-if)# interface Fast Ethernet 0/1/1
Router(config-if)# switchport access vlan 2
Router(config-if)# exit
```

VLAN Trunking Using VTP Example

The following example shows how to configure the switch as a VTP server:

```
Router# vlan database
Router(vlan)# vtp server
Setting device to VTP SERVER mode.
Router(vlan)# vtp domain Lab
```

```
_Network
Setting VTP domain name to Lab_Network
Router(vlan)# vtp password WATER
Setting device VLAN database password to WATER.
Router(vlan)# exit
APPLY completed.
Exiting....
Router#
```

The following example shows how to configure the switch as a VTP client:

```
Router# vlan database
Router(vlan)# vtp client
Setting device to VTP CLIENT mode.
Router(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....
Router#
```

The following example shows how to configure the switch as VTP transparent:

```
Router# vlan database
Router(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
Router(vlan)# exit
APPLY completed.
Exiting....
Router#
```

Spanning Tree Examples

- Spanning-Tree Interface and Spanning-Tree Port Priority: Example, page 95
- Spanning-Tree Port Cost: Example, page 95
- Bridge Priority of a VLAN: Example, page 96
- Hello Time: Example, page 96
- Forward-Delay Time for a VLAN: Example, page 96
- Maximum Aging Time for a VLAN: Example, page 96
- Spanning Tree: Examples, page 96
- Spanning Tree Root: Example, page 97
- Spanning-Tree Interface and Spanning-Tree Port Priority Example, page 108
- Spanning-Tree Port Cost Example, page 109
- Bridge Priority of a VLAN Example, page 110
- Hello Time Example, page 110
- Forward-Delay Time for a VLAN Example, page 110
- Maximum Aging Time for a VLAN Example, page 110
- Spanning Tree Examples, page 111
- Spanning Tree Root Example, page 111

Spanning-Tree Interface and Spanning-Tree Port Priority Example

The following example shows the VLAN port priority of an interface being configured:

```
Router# configure terminal

Router(config)# interface fastethernet 0/3
/2
Router(config-if)# spanning
```

```
-
tree vlan 20 port
-priority 64

Router(config-if)# end

Router#
```

The following example shows how to verify the configuration of VLAN 200 on the interface when it is configured as a trunk port:

```
Router# show spanning
-
tree vlan 20
 VLAN20 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00ff.ff90.3f54
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 00ff.ff10.37b7
  Root port is 33 (FastEthernet0/3/2), cost of root path is 19
  Topology change flag not set, detected flag not set
  Number of topology flags 0 last change occurred 00:05:50 ago
  Times: hold 1, topology change 35, notification 2
     hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 0
 Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding
  Port path cost 18, Port priority 64, Port Identifier 64.33
  Designated root has priority 32768, address 00ff.ff10.37b7
  Designated bridge has priority 32768, address 00ff.ff10.37b7
  Designated port id is 128.13, designated path cost 0
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 1, received 175
Router#
```

Spanning-Tree Port Cost Example

The following example shows how to change the spanning-tree port cost of a Fast Ethernet interface:

```
Router# configure terminal

Router(config)# interface fastethernet
0/3/2
Router(config-if)# spanning
-
tree cost 18
Router(config-if)# end

Router#
Router# show run interface fastethernet0/3/2
Building configuration...
Current configuration: 140 bytes
!
interface FastEthernet0/3/2
 switchport access vlan 20
  no ip address
  spanning-tree vlan 20 port-priority 64
  spanning-tree cost 18
end
```

The following example shows how to verify the configuration of the interface when it is configured as an access port:

```
Router# show spanning
-
tree interface fastethernet 0/3
/2
 Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding
  Port path cost 18, Port priority 64, Port Identifier 64.33
  Designated root has priority 32768, address 00ff.ff10.37b7
```

```
  Designated bridge has priority 32768, address 00ff.ff10.37b7
  Designated port id is 128.13, designated path cost 0
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 1, received 175
Router#
```

Bridge Priority of a VLAN Example

The following example shows the bridge priority of VLAN 20 being configured to 33792:

```
Router# configure terminal
Router(config)# spanning
-
tree vlan 20 priority 33792

Router(config)# end

Router#
```

Hello Time Example

The following example shows the hello time for VLAN 20 being configured to 7 seconds:

```
Router# configure terminal

Router(config)# spanning
-
tree vlan 20
hello-
time 7

Router(config)# end

Router#
```

Forward-Delay Time for a VLAN Example

The following example shows the forward delay time for VLAN 20 being configured to 21 seconds:

```
Router# configure terminal

Router(config)# spanning
-
tree vlan 20 forward-time 21

Router(config)# end

Router#
```

Maximum Aging Time for a VLAN Example

The following example configures the maximum aging time for VLAN 20 to 36 seconds:

```
Router# configure terminal

Router(config)# spanning
-
tree
 vlan 20 max
-age 36

Router(config)# end
```

```
Router#
```

Spanning Tree Examples

The following example shows spanning tree being enabled on VLAN 20:

```
Router# configure terminal
Router(config)# spanning
-
tree
 vlan
 20

Router(config)# end

Router#
```

Note Because spanning tree is enabled by default, issuing a **show running** command to view the resulting configuration will not display the command you entered to enable spanning tree.

The following example shows spanning tree being disabled on VLAN 20:

```
Router# configure
 terminal

Router(config)# no
 spanning
-tree
 vlan
 20

Router(config)# end

Router#
```

Spanning Tree Root Example

The following example shows the switch being configured as the root bridge for VLAN 10, with a network diameter of 4:

```
Router#
configure terminal

Router(config)#
spanning-tree vlan 10 root primary diameter 4

Router(config)#
exit

Router#
```

MAC Table Manipulation Example

The following example shows a static entry being configured in the MAC address table:

```
Router(config)#
mac-address-table static beef.beef.beef interface fastethernet 0/1/5
Router(config)#
end
```

The following example shows port security being configured in the MAC address table.

```
Router(config)# mac-address-table secure 0000.1111.2222 fastethernet 0/1/2 vlan 3
Router(config)# end
```

Switched Port Analyzer (SPAN) Source Examples

- SPAN Source Configuration: Example, page 97
- SPAN Destination Configuration: Example, page 98
- Removing Sources or Destinations from a SPAN Session: Example, page 98
- SPAN Source Configuration Example, page 112
- SPAN Destination Configuration Example, page 112
- Removing Sources or Destinations from a SPAN Session Example, page 112

SPAN Source Configuration Example

The following example shows SPAN session 1 being configured to monitor bidirectional traffic from source interface Fast Ethernet 0/1/1:

```
Router(config)# monitor session 1 source interface fastethernet 0/1
/1
```

SPAN Destination Configuration Example

The following example shows interface Fast Ethernet 0/3/7 being configured as the destination for SPAN session 1:

```
Router(config)# monitor session 1 destination interface fastethernet 0/3/7
```

Removing Sources or Destinations from a SPAN Session Example

This following example shows interface Fast Ethernet 0/3/2 being removed as a SPAN source for SPAN session 1:

```
Router(config)# no monitor session 1 source interface fastethernet 0/3/2
```

IGMP Snooping Example

The following example shows the output from configuring IGMP snooping:

```
Router# show mac-address-table multicast igmp-snooping
HWIC Slot: 1
--------------
    MACADDR     VLANID     INTERFACES
0100.5e05.0505    1        Fa0/1/1
0100.5e06.0606    2
HWIC Slot: 3
--------------
    MACADDR     VLANID     INTERFACES
0100.5e05.0505    1        Fa0/3/4
0100.5e06.0606    2        Fa0/3/0
Router#
```

The following is an example of output from the **show running interface**privileged EXEC command for VLAN 1:

```
Router#
show running interface vlan 1
Building configuration...
Current configuration :82 bytes
!
interface Vlan1
 ip address 192.168.4.90 255.255.255.0
 ip pim sparse-mode
end
Router#
show running interface vlan 2

Building configuration...
Current configuration :82 bytes
!
interface Vlan2
 ip address 192.168.5.90 255.255.255.0
 ip pim sparse-mode
end
Router#
Router# show ip igmp group
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
209.165.200.225 Vlan1                    01:06:40  00:02:20  192.168.41.101
209.165.200.226 Vlan2                    01:07:50  00:02:17  192.168.5.90
209.165.200.227 Vlan1                    01:06:37  00:02:25  192.168.41.100
209.165.200.228 Vlan2                    01:07:40  00:02:21  192.168.31.100
209.165.200.229 Vlan1                    01:06:36  00:02:22  192.168.41.101
209.165.200.230 Vlan2                    01:06:39  00:02:20  192.168.31.101
Router#
Router# show ip mroute
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C -
Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode
(*, 209.165.200.230), 01:06:43/00:02:17, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:43/00:02:17
(*, 209.165.200.226), 01:12:42/00:00:00, RP 0.0.0.0, flags:DCL
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan2, Forward/Sparse, 01:07:53/00:02:14
(*, 209.165.200.227), 01:07:43/00:02:22, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:40/00:02:22
    Vlan2, Forward/Sparse, 01:07:44/00:02:17
```

(*, 209.165.200.2282), 01:06:43/00:02:18, RP 0.0.0.0, flags:DC

```
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:40/00:02:18
    Vlan2, Forward/Sparse, 01:06:43/00:02:16
Router#
```

Storm-Control Example

The following example shows bandwidth-based multicast suppression being enabled at 70 percent on Fast Ethernet interface 2:

```
Router# configure terminal
Router(config)# interface FastEthernet0/3/3
Router(config-if)# storm-control multicast threshold 70.0 30.0
Router(config-if)# end
Router# show storm-control multicast
Interface  Filter State  Upper    Lower    Current
---------  ------------  -----    -----    -------
Fa0/1/0    inactive      100.00%  100.00%  N/A
Fa0/1/1    inactive      100.00%  100.00%  N/A
Fa0/1/2    inactive      100.00%  100.00%  N/A
Fa0/1/3    inactive      100.00%  100.00%  N/A
Fa0/3/0    inactive      100.00%  100.00%  N/A
Fa0/3/1    inactive      100.00%  100.00%  N/A
Fa0/3/2    inactive      100.00%  100.00%  N/A
Fa0/3/3    Forwarding     70.00%   30.00%  0.00%
Fa0/3/4    inactive      100.00%  100.00%  N/A
Fa0/3/5    inactive      100.00%  100.00%  N/A
Fa0/3/6    inactive      100.00%  100.00%  N/A
Fa0/3/7    inactive      100.00%  100.00%  N/A
Fa0/3/8    inactive      100.00%  100.00%  N/A
```

Ethernet Switching Examples

- Subnets for Voice and Data: Example, page 100
- Inter-VLAN Routing: Example, page 101
- Single Subnet Configuration: Example, page 101
- Ethernet Ports on IP Phones with Multiple Ports: Example, page 101

- Subnets for Voice and Data Example, page 114
- Inter-VLAN Routing Example, page 115
- Single Subnet Configuration Example, page 115
- Ethernet Ports on IP Phones with Multiple Ports Example, page 115

Subnets for Voice and Data Example

The following example shows separate subnets being configured for voice and data on the EtherSwitch HWIC:

```
interface FastEthernet0/1/1
 description DOT1Q port to IP Phone
 switchport native vlan 50
 switchport mode trunk
 switchport voice vlan 150
interface Vlan 150
description voice vlan
ip address
209.165.200.227
 255.255.255.0
ip helper-address
209.165.200.228
 (See Note below)
interface Vlan 50
description data vlan
ip address
```

```
209.165.200.220
 255.255.255.0
```

This configuration instructs the IP phone to generate a packet with an 802.1Q VLAN ID of 150 with an 802.1p value of 5 (default for voice bearer traffic).

Note In a centralized CallManager deployment model, the DHCP server might be located across the WAN link. If so, an **ip helper-address** command pointing to the DHCP server should be included on the voice VLAN interface for the IP phone. This is done to obtain its IP address as well as the address of the TFTP server required for its configuration.

Be aware that IOS supports a DHCP server function. If this function is used, the EtherSwitch HWIC serves as a local DHCP server and a helper address would not be required.

Inter-VLAN Routing Example

Configuring inter-VLAN routing is identical to the configuration on an EtherSwitch HWIC with an MSFC. Configuring an interface for WAN routing is consistent with other IOS platforms.

The following example provides a sample configuration:

```
interface Vlan 160
 description voice vlan
 ip address 10.6.1.1 255.255.255.0
interface Vlan 60
 description data vlan
 ip address 10.60.1.1 255.255.255.0
interface Serial0/3/0
 ip address 172.3.1.2 255.255.255.0
```

Note Standard IGP routing protocols such as RIP, IGRP, EIGRP, and OSPF are supported on the EtherSwitch HWIC. Multicast routing is also supported for PIM dense mode, sparse mode and sparse-dense mode.

Single Subnet Configuration Example

The EtherSwitch HWIC supports the use of an 802.1p-only option when configuring the voice VLAN. Using this option allows the IP phone to tag VoIP packets with a Cost of Service of 5 on the native VLAN, while all PC data traffic is sent untagged.

The following example shows a single subnet configuration for the EtherSwitch HWIC:

```
Router# FastEthernet 0/1/2
description Port to IP Phone in single subnet
 switchport access vlan 40
```

The EtherSwitch HWIC instructs the IP phone to generate an 802.1Q frame with a null VLAN ID value but with an 802.1p value (default is COS of 5 for bearer traffic). The voice and data VLANs are both 40 in this example.

Ethernet Ports on IP Phones with Multiple Ports Example

The following example illustrates the configuration for the IP phone:

```
interface FastEthernet0/x/x
```

```
 switchport voice vlan x
 switchport mode trunk
```

The following example illustrates the configuration for the PC:

```
interface FastEthernet0/x/y
 switchport mode access
 switchport access vlan y
```

Note Using a separate subnet, and possibly a separate IP address space, may not be an option for some small branch offices due to the IP routing configuration. If the IP routing can handle an additional subnet at the remote branch, you can use Cisco Network Registrar and secondary addressing.

Additional References

The following sections provide references related to EtherSwitch HWICs.

Related Documents

Related Topic	Document Title
IP LAN switching commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS LAN Switching Services Command Reference*
Bridge-related commands; complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Bridge Command Reference*
Information about configuring Voice over IP features	Cisco IOS Voice Configuration Library
Voice over IP commands	*Cisco IOS Voice Command Reference*
Information about configuring IP routing	*Cisco IOS IP Routing: Protocol-Independent Configuration Guide* for the Cisco IOS Release you are using
Information about intrachassis stacking configuration	16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series module
VLAN concepts	”VLANs” section of the EtherSwitch Network Module
Inline power for Cisco IP phones concepts	“Inline Power for Cisco IP Phones” section of the EtherSwitch Network Module
Layer 2 Ethernet switching concepts	“Layer 2 Ethernet Switching” section of the EtherSwitch Network Module

Related Topic	Document Title
802.1x authentication concepts	“802.1x Authentication” section of the EtherSwitch Network Module
Spanning tree protocol concepts	“Using the Spanning Tree Protocol with the EtherSwitch Network Module” section of the EtherSwitch Network Module
Cisco Discovery Protocol concepts	“Cisco Discovery Protocol” section of the EtherSwitch Network Module
Switch port analyzer concepts	“Switched Port Analyzer” section of the EtherSwitch Network Module
IGMP snooping concepts	IGMP Snooping” section of the EtherSwitch Network Module
Storm control concepts	“Storm Control” section of the EtherSwitch Network Module
Intrachassis stacking concepts	‘Intrachassis Stacking” section of the EtherSwitch Network Module
Fallback bridging concepts	“Fallback Bridging” section of the EtherSwitch Network Module

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards have not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the Cisco HWIC-4ESW and the Cisco HWIC-D-9ESW EtherSwitch Cards

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 Feature Information for the 4-Port Cisco HWIC-4ESW and the 9-Port Cisco HWIC-D-9ESW EtherSwitch High Speed WAN Interface Cards

Feature Name	Releases	Feature Information
4-port Cisco HWIC-4ESW and the 9-port Cisco HWIC-D-9ESW EtherSwitch high speed WAN interface cards (HWICs) hardware feature	12.3(8)T4	The 4-port Cisco HWIC-4ESW and the 9-port Cisco HWIC-D-9ESW EtherSwitch high speed WAN interface cards (HWICs) hardware feature is supported on Cisco 1800 (modular), Cisco 2800, and Cisco 3800 series integrated services routers. Cisco EtherSwitch HWICs are 10/100BASE-T Layer 2 Ethernet switches with Layer 3 routing capability. (Layer 3 routing is forwarded to the host and is not actually performed at the switch.) Traffic between different VLANs on a switch is routed through the router platform. Any one port on a Cisco EtherSwitch HWIC may be configured as a stacking port to link to another Cisco EtherSwitch HWIC or EtherSwitch network module in the same system. An optional power module can also be added to provide inline power for IP telephones. The HWIC-D-9ESW HWIC requires a double-wide card slot.